draft-zuniga-mac-address-randomization-00

Amelia Andersdotter, CENTR

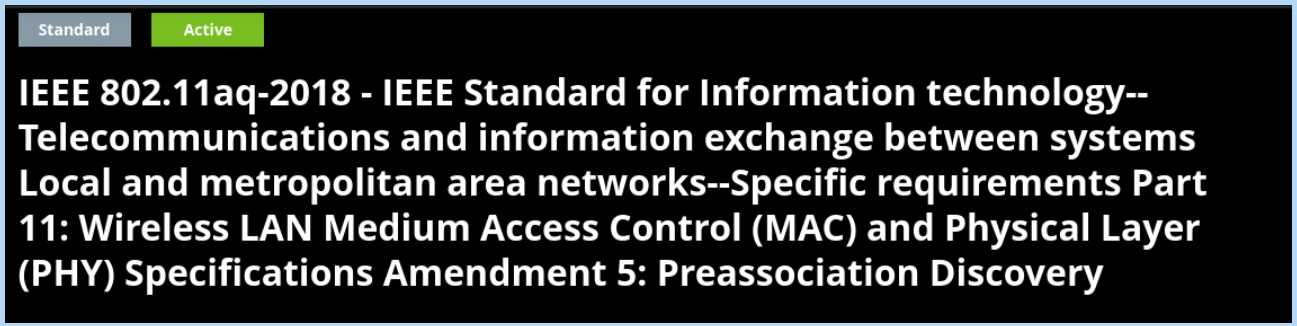
IETF109, November 2020

- Privacy increasing concern
  - Layer-2 identifiers (MAC addresses) have been assigned uniquely to devices and are transmitted in the clear in, for instance, beacons, probe requests, or after association.
  - MAC addresses can easily be intercepted and used to track location or behaviour.
- Several projects in IETF, IEEE 802 and among mobile OS vendors to deal with plain-text, unique, permanent MAC addresses
  - Assigning a random MAC address to a device per connection, per SSID, after some time period
  - Area of extensive research (see reference Martin et al (2017) in draft for more comprehensive list of research in this area, or IEEE 802.11 RCM TIG final report in 11-19/1442r9, also in draft).

- Early work as far as back as IETF91
  - Joint W3C/IAB privacy tutorial
  - Testing MAC randomization and technical features (i.e. collisions, dhcp, etc.)
  - Thoroughly documented
- Led to a number of other initiatives (see draft)
- MAC randomization is now a default privacy feature in major mobile OS (see last slide)

- IETF work inspired a new privacy research project, P802E.
  - Study group phase to map privacy in different IEEE 802 standards (link to document repository with associated studies in draft)
  - Recommended Practice for Privacy Considerations for IEEE 802 Technologies finalized during autumn 2020.
- Discussions about randomized MAC for different types of devices (industrial, sensors, personal, etc.) in e.g. 802C ("SLAP")

- IEEE 802.11aq amendment from 2018 introducing robust recommendations for MAC randomizations.
- New work proposed (potential future IEEE 802.11bh and .11bi to look at privacy features, and network operation in absence of clear-text permanent layer 2 identifiers (see draft).
  - Will look at alternatives to layer 2 identifier mechanisms and general layer 2 privacy mechanisms



- Relying on higher-layer identity management (Passpoint (WFA), OpenRoaming (WBA))
  - Uses e.g. RADIUS
  - cf. eduroam architecture (RFC7593)
- Stepping up efforts in this field since 2020, together with operators.

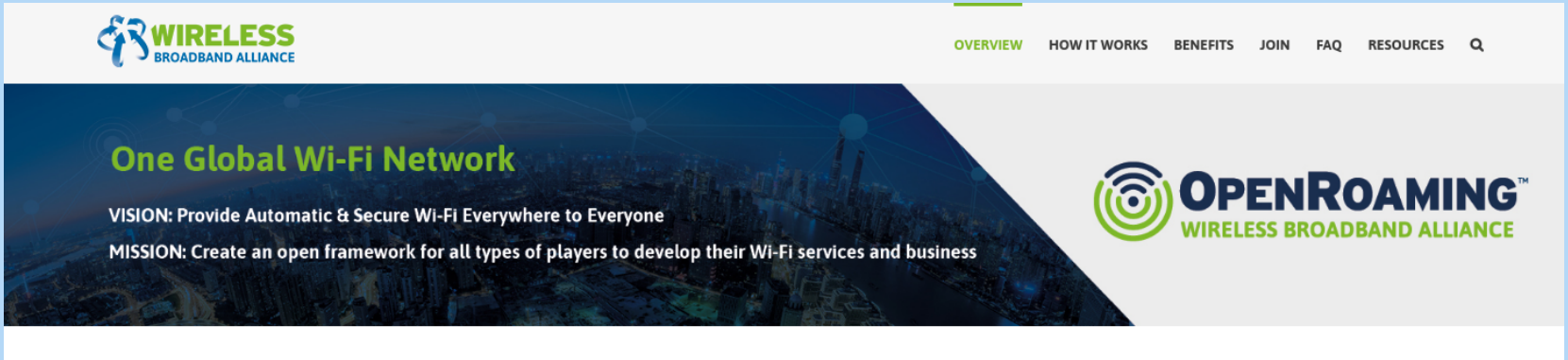


Table from: https://www.fing.com/news/private-mac-address-on-ios-14

Android 10+	iOS 14+
The randomised MAC address is bound to the network name (SSID) and it does not change when connecting to a different access point with the same name.	**The randomised MAC address is bound to the access point identifier (BSSID)** so it will change when connecting to a different access point with the same name.
The randomised MAC address is stable across reconnections and won't change over time for the same network.	**The randomised MAC address is not stable** and it will change every now and then even if the iOS device remains connected to the same network. The MAC address refresh rate is not known, but from our tests we verified that it may change several times in the same day.
The randomised MAC address is reset when the device forgets a WiFi network. Upon a new connection a new randomised MAC address will be generated.	**The randomised MAC address is reset when the device forgets a WiFi network.** Upon a new connection a new randomised MAC address will be generated.
MAC address randomisation is enabled by default for all the new WiFi networks. If the device previously connected to a WiFi network identifying itself with the real MAC address, no randomised MAC address will be used (unless manually enabled).	**MAC address randomisation is enabled by default for all the WiFi networks**, even for WiFi networks to which the device previously connected, identifying itself with the real MAC address.

* Microsoft Windows will be covered in the next presentation

Comments? Questions?

See also:

`https://datatracker.ietf.org/doc/draft-zuniga-mac-address-randomization/`